EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
Facsimile: (573) 659-4460

Co-Lead Counsel on behalf of Plaintiffs

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: NICKELODEON CONSUMER PRIVACY LITIGATION	**MDL No. 2443**
	Docket No. 2:12-cv-07829 (SRC)(CLW)
THIS DOCUMENT RELATES TO:	**ECF Case**
ALL ACTIONS	**Oral Argument Requested**

PLAINTIFFS' BRIEF IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS

TO:

Jeffrey J. Greenbaum
Joshua N. Howley
SILLS CUMMIS & GROSS, P.C.
One Riverfront Plaza
Newark, NJ 07102

Colleen Bal
Michael Rubin
Tonia Klausner
WILSON SONSINI GOODRICH & ROSATI, PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105

Stephen M. Orlofsky
BLANK ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540

Bruce P. Keller
Jeffrey S. Jacobson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Secondary Authorities

INTRODUCTION

On July 2, 2014, this Court sustained Defendants' Motion To Dismiss and granted Plaintiffs leave to amend three claims:

- the Video Privacy Protection Act ("VPPA") claim against Defendant Viacom;
- the New Jersey Computer Related Offenses Act ("NJCROA") claim against Defendant Viacom; and
- the Intrusion Upon Seclusion claim against Defendants Viacom and Google.

Plaintiffs' Second Consolidated Class Action Complaint sets forth a more detailed factual narrative with respect to each of these claims and exceeds the pleading mandate established by this Court's prior Order. In particular, the Second CAC includes additional allegation details: (1) Viacom's unlawful dissemination to Google of information specifically identifying Plaintiffs, in violation of the VPPA and NJCROA; and (2) the "highly offensive" nature of Defendants' intentional intrusion into the private matters of children, which constitutes an intrusion upon the seclusion of minor children.

These new allegations raise plausible claims and issues of fact which cannot be resolved at the pleading stage. For the reasons more fully set forth below, Defendants' motions should be denied.

STATEMENT OF FACTS

I. THE UNDERLYING ALLEGATIONS CONCERNING WHAT VIACOM DISCLOSES TO GOOGLE BY WAY OF THE DOUBLECLICK COOKIES

Defendant Viacom permits and facilitates the placement of Defendant Google's DoubleClick cookies on the browsers of the Plaintiffs, all Internet users known by both

Defendants to be minor children under the age of 13. [1] Through these cookies, Defendant Viacom disclosed at least the following information about the Plaintiffs and their Internet communications to Google: (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's Nick.com website; and (11) the DoubleClick persistent cookie identifiers. Second CAC at ¶143.

a. THE ADDITIONAL SPECIFIC FACTS DEMONSTRATING HOW THIS INFORMATION IDENTIFIES CHILDREN

The information disclosed by Viacom constitutes identifiable information not only by its content – but more importantly because of its recipient. Information that might be anonymous to the average person or business is not anonymous to Google. Because of its Internet ubiquity, Google owns the equivalent of a modern-day Enigma machine that personally identifies Internet users via persistent cookie identifiers, IP addresses, and unique device identifiers.

Google is the global epicenter of Internet search and browsing. Second CAC at ¶18. To maintain that position of supremacy, Google owns a wide array of services from which it collects the personal information of Internet users. Second CAC at ¶¶ 80-85. Its eponymous search engine processes more than 12 billion Internet searches a month and nearly 70 percent of all searches in the United States. Second CAC at ¶81(b). It operates the world's third most-popular social network at plus.google.com, which boasts more than 300 million members. Second CAC

[1] Plaintiffs note that their original CAC included a class of all users of the websites Nick.com, NickJr.com, and NeoPets.com. In their Second CAC, Plaintiffs have only alleged a class of users of Nick.com.

at ¶81a. Google hosts Gmail, an email service with more than 250 million users. Second CAC at ¶81c. It owns YouTube, the world's most popular Internet video service, which shows more than 150 million videos each month to Internet users. Second CAC at ¶81d. It runs Google Maps, the world's most popular mapping service and, according to some estimates, the world's most popular smart-phone app. Second CAC at ¶81e. Google also operates (a) Android, the world's most popular mobile phone platform, (b) its own web-browser called Google Chrome, (c) an online software suite called Google Apps that is used by 66 of the top 100 universities in the United States, governments in 45 states, and 5 million businesses; (d) an online photography website - Picasa; and (e) an electronic store called Play. Second CAC at ¶81f-j.

Taken together, these services collect more information about consumers than even the Internet Service Providers who provide their access to the Internet. Second CAC at ¶93. This information includes, but is not limited to: (a) first and last names; (b) home or other physical addresses; (c) precise locations of users through GPS; (d) IP addresses; (e) telephone numbers; (f) lists of contacts; (g) the content of Gmail users' Gmail messages; (h) search history at Google.com and YouTube; (i) web-surfing histories; (j) Android device activity; and (k) all activity on Google's social network called Google Plus. Second CAC at ¶93. All of the Google services collect user IP address, unique device identifiers, and user account information. Second CAC at ¶82.

Google's ubiquity is amplified by DoubleClick. In October 2012, DoubleClick cookies were present on 69 of the 100 most popular websites. Second CAC at ¶81. In total, experts estimate Google's servers (which facilitate the businesses listed above and DoubleClick) account for 25 percent of all Internet traffic in North America, an amount larger than the combined traffic of Facebook, Netflix, and Instagram. Second CAC at ¶81.

Defendant Google employs persistent cookies to track users across its various properties and the Internet. Second CAC at ¶82. Google's social network Google+ tracks users with the same persistent DoubleClick cookie it uses for Nick.com and with Google+ cookies. Second CAC at ¶82(a). Google also tracks YouTube users with the same persistent DoubleClick cookies it uses for Nick.com, Google+ cookies, and cookies from the domain clients6.google.com. Second CAC at ¶82d. Google's eponymous search engine tracks users with cookies from Google+ and other domains. Second CAC at ¶82b. Gmail tracks users with Google+ and other cookies. Second CAC at ¶82c.

In light of the enormity of these efforts, when Viacom provides the DoubleClick data to Google, the information about the Internet users becomes unique, identifiable and valuable. Indeed, Google informs users that it collects "device-specific information (such as [a user's] hardware model, operating system version, unique device identifiers, and mobile network information including phone number" and "may associate device identifiers … with [a user's] Google account." Second CAC at ¶85a.

Google also "automatically collect[s] and store[s] certain information in server logs[, which] may include … search queries, … Internet protocol address, … device event information such as … hardware settings, browser-type, browser language, the date and time of your request and referral URL," and "cookies that may uniquely identify your browser or your Google account." Second CAC at ¶85b.

Defendant Google further admits that IP addresses and cookie information are not anonymous to the company. In order to "anonymize" user records, Google promises to scrub its databased after nine to 18 months:

> Like most websites, our servers automatically record the page requests made when users visit our sites. These server logs typically include your web request, IP

> address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons[.] … We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months).

Second CAC at ¶91. Defendant Google's former Privacy Director admitted that, with the information Google has in its possession, IP addresses are personally-identifying:

> A black-and-white declaration that all IP addresses are always personal data incorrectly suggests that every IP address can be associated with a specific individual. In some contexts this is more true: if you're an ISP and you assign an IP address to a computer that connects under a particular subscriber's account, and you know the name and address of the person who holds that account, then that IP address is more like personal data, even though multiple people could still be using it. On the other hand, the IP addresses recorded by every website on the planet without additional information should not be considered personal data, because these websites usually cannot identify the human beings behind those number strings.

Second CAC at ¶92.

By design, Google is no ordinary website. In fact, it keeps more information on its users than many ISPs. Second CAC at ¶93. In addition, Viacom is aware of Google's ubiquity and ability to identify Internet users via the information Viacom discloses to it. Second CAC ¶¶95-96. In light of the information that Google already has in its possession, the data provided by Viacom enables Google to ascertain the specific identities of its users.

II. NEWLY-PLEADED FACTS RELATING TO THE "HIGHLY OFFENSIVE" ELEMENT OF INTRUSION UPON SECLUSION

Whether an act is "highly offensive" is determined by social norms which can be found from various sources including, but not limited to, criminal and civil laws, industry standards and general public opinion. Plaintiffs' Second CAC pleads facts which show Defendants' conduct violated social norms as expressed (1) directly by public policy in the form of civil and criminal laws designed to protect privacy, (2) by the standards of Defendants' own industry, and (3) by public opinion.

Specifically, Plaintiffs allege facts showing the Defendants violated the VPPA, the Wiretap Act (or, in the alternative, the Pen Register Act), and the Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states. Second CAC at ¶160. Plaintiffs allege violation of the Terms of Use of Internet Service Providers and web-browsers, and of the standards of the online advertising industry. Second CAC at ¶163 and ¶167.

Eighty-six percent of Americans oppose the practice of advertisers tracking of "a child's behavior online even if they give the child free content." Second CAC at ¶164b. Eighty percent oppose the tracking of children even where an advertiser does not "know a child's name and address[.]" Second CAC at ¶164c. Ninety-one percent believe advertisers should receive a parent's permission before placing tracking software on a minor child's computing device. Second CAC at ¶164d. Ninety percent support federal law requiring parental permission before the collection of personal information of a minor child online. Second CAC at ¶164e.

Defendants' self-praise to the contrary, Americans do not generally approve of their behavior even when it regards tracking adults. Nearly 85 percent are "alarmed" by "advertisers and companies tracking … behavior across the web." Second CAC at ¶164g. Nearly 70 percent are concerned about the collection of digital information from their computers or phones by government or private companies. Second CAC at ¶164h. Nearly 78 percent oppose having their "online behavior tracked and analyzed." Second CAC at ¶164i. The underlying message from these polls is clear: what the Defendants do here is highly offensive, and a reasonable person such as a juror would agree.

Defendants' illegal tracking is made worse by its scope. The invasions of privacy were perpetrated millions of times on minor children. Second CAC at ¶165. And, the targeting of children was more intrusive than traditional Internet tracking of adults. Second CAC at ¶166.

LEGAL ARGUMENT

I. PLAINTIFFS HAVE STATED A CLAIM AGAINST VIACOM UNDER THE VIDEO PRIVACY PROTECTION ACT

a. PERSONALLY IDENTIFIABLE INFORMATION UNDER THE VPPA

The Video Privacy Protection Act prohibits video-tape service providers, such as Viacom, from disclosing to third parties "personally-identifiable information" regarding its customers without the customer's consent. 18 U.S.C. § 2710.[2]

The VPPA reflects Congress' intent that "personally-identifiable information" be broadly defined to include, at a minimum, "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). The original Senate Report explains:

> The term 'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider. Unlike other definitions in this subsection, paragraph (a)(3) uses the word 'includes' ***to establish a minimum, but not exclusive, definition of personally identifiable information***.

S. Rep. 100-599 at 12 (1988) (emphasis added). This *minimum, but not exclusive definition* takes account of changing realities based on advances in technology. Furthermore, as this Court explained in its prior Order, the VPPA must be read to "comport with common sense – 'a person can be identified by more than just their name and address.'" See *In re Nickelodeon*, MDL No. 2443, 2014 WL 3012873, at *19 (D.N.J. July 2, 2014) (citing *In re Hulu*, No. C11-03764, 2014 WL 1724344, at *11 (N.D. Cal., April 28, 2014) ("One can be identified in many ways: by a

[2] In a footnote to its Memorandum of Law, Defendant Viacom mentions three arguments previously rejected by this Court: (1) Plaintiffs lack Article III standing; (2) Plaintiffs are not "aggrieved" within the meaning of the VPPA; and (3) Viacom is not a "video tape service provider." Doc. 77-1, Viacom Memo. at 17, n.5. In response, Plaintiffs incorporate their prior arguments and the Court's prior rulings on these arguments.

picture, by pointing, by an employee number, by the station or office or cubicle where one works . . . .")).

Consistent with the VPPA, other federal statutes and regulations similarly define PII broadly. For example:

- The Federal Trade Commission defines "personal information" to include "online contact information" and "persistent identifier[s] that can be used to recognize a user over time and across different Web sites or online services," including, but not limited to "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier." 16 C.F.R. §312.
- The Department of Homeland Security defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual."[3]
- The Gramm-Leach Financial Modernization Act of 1999, 15 U.S.C. § 6802, prohibits disclosures by financial institutions of consumers' "non-public personal information," which the Securities and Exchange Commission has interpreted as including "any information [collected] through an Internet 'cookie' (an information collecting device from a web server)." 17 C.F.R. § 248.3.
- The Federal Education Rights and Privacy Act (FERPA) and the regulations promulgated thereunder prohibit the release of "personally identifiable information" without the written consent of a child's parents, including:

  (a) the name and address of the student, the student's parent or other family members;

  (b) direct personal identifiers, such as the student's social security number, student number, or biometric record;

  (c) indirect identifiers, such as the student's date of birth;

  (d) other information that, alone or in combination, is linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and

  (e) information requested by a person who the educational institution reasonably believes knows the identity of the student.

  20 U.S.C. § 1232(g)(b)(1); 34 C.F.R. § 99.3.

[3] Available at http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf. Last visited Oct. 16, 2014.

- The Children's Online Privacy Protection Act (COPPA) and the regulations promulgated thereunder define personal information as "individually identifiable information" including: first and last names; screen or user names; physical and email addresses; persistent identifiers that can be used to recognize a user over time and across different Web sites or online services, such as customer numbers held in cookies, IP addresses, processor or device serial numbers, or unique device identifiers; any other information that permits the contacting of specific individuals; and information concerning the child or parent collected and combined with the above identifiers. 15 U.S.C. § 6501(8); 16 C.F.R. §312.2.

The technology industry itself defines personally identifiable information broadly, with Google defining "personal information" to include "information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google."[4] More specifically, Viacom and Google, as members of the Interactive Advertising Bureau, have agreed to IAB's Code of Conduct, which mandates that members "not collect 'personal information' as defined in [COPPA], from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising." [5]

As illustrated below and in the Second CAC, the materials disclosed by Viacom fall within this definition, and the VPPA Cause of Action should proceed.

b. PLAINTIFFS ADEQUATELY ALLEGE THAT DEFENDANT VIACOM HAS DISCLOSED 'PERSONALLY IDENTIFIABLE INFORMATION' TO GOOGLE

In its previous Order, this Court ruled that the information allegedly disclosed "might one day serve as the basis of personal identification after some effort on the part of the recipient, but

[4] See http://www.google.com/policies/privacy/key-terms/#toc-terms-personal-info. Last visited Oct. 15, 2014.
[5] http://www.iab.net/media/file/IAB_Code_of_Conduct_10282-2.pdf at 2.

the same could be said for nearly any type of personal information; this Court reads the VPPA to require a more tangible, immediate link." Doc. 65, Opinion at 22.

Plaintiffs' Second CAC provides that "tangible, immediate link." Plaintiffs allege that Viacom, with knowledge of Google's unique ability to link information to identify individuals, disclosed the following information to Google: (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications; and (11) the DoubleClick persistent cookie identifiers. Second CAC at ¶143. Given the quantity and nature of information that Google already has in its possession, Plaintiffs further allege that this information is sufficient to link specific persons with their video viewing requests and histories. Second CAC at ¶144. This conduct personally identifies the user, and violates the VPPA.

Despite these allegations, Viacom still claims that DoubleClick cookies are "anonymous" because there is no tangible, immediate link to the identity of actual people. Doc. 77-1, Viacom Memo. at 10-15. In doing so, Viacom relies on *In re Hulu*, No. C11-03764, 2014 WL 1724344 (N.D. Cal., April 28, 2014) and *Ellis v. Cartoon Network*, No. 1:14-cv-00484, 2014 WL 5023535 (N.D. Ga. Oct. 8, 2014). Such reliance is misplaced, because *Hulu* and *Ellis* demonstrate that what Viacom has done here is unlawful.

In *Hulu*, the Court found liability for the disclosure of persistent cookie identifiers to Facebook which, like Google, had the ability to link the information received from Hulu to specific individuals using the information already in Facebook's possession. *In re Hulu*, No. C11-03764, 2014 WL 1724344, at *13-17 (N.D. Cal., April 28, 2014). The Court did not find liability for disclosures to comScore, a third-party analytics company that lacked the independent

ability to link personally identifiable information of Internet users from other sources. Id. at *12. Similarly, in *Ellis*, the Court found no liability for disclosure of unique device identifiers to a third-party company called Bango which, like comScore, lacked the ability to link the identifiers received to specific consumers. *Ellis v. Cartoon Network*, No. 1:14-cv-00484, 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014).

Here, Plaintiffs allege that Google is able to link the information received from Viacom to specific individuals by utilizing the information already in Google's possession. As Plaintiffs' Second CAC makes clear, "Google has, by design, become the global epicenter of Internet search and browsing activity." Second CAC at ¶18. Google has its own social media website called Google+ from which it tracks the communications of Internet users with various persistent cookie identifiers, including the very DoubleClick cookies at issue in this case. Second CAC at ¶¶80(a), 91.

Unlike comScore or Bango, Google is ubiquitous. Its Internet traffic dwarfs all other companies, including Facebook, and accounts for 25 percent of all Internet traffic in North America – more than Facebook, Netflix, and Instagram combined. Second CAC at ¶81. Through its various means, Google directly "collects users' IP addresses, unique device identifiers, and user account" information. Second CAC at ¶80. It tracks users on Google+ and YouTube using the same DoubleClick persistent identifiers that it uses to track them on Nick.com and other websites. Second CAC at ¶80(a) and (d). Other Google services track users with cookies from the main Google.com domain and from Google+. Second CAC at ¶80(a) and (d). Google's other services, including Gmail and Google+, collect user's first and last names, hometowns, email addresses, and other information. Second CAC at ¶81.

Moreover, Google admits that it connects persistent cookie identifiers, IP addresses, and unique device identifiers with user account information. Second CAC at ¶83. Google further publicly admits that, for Google, IP addresses and cookie information are not "anonymous" as claimed by Viacom. Second CAC at ¶89 ("[Google's] server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. . . . We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months)."). Indeed, Google's own Privacy Policy defines "personal information" in a manner that would include IP addresses and cookie identifiers, defining it as "information which you provide to us which personally identifies you, such as your name, email address or billing information, ***or other data which can be reasonably linked to such information by Google***."[6]

Plaintiffs allege that Google combines IP addresses, unique device identifiers, and other information collected in association with its DoubleClick cookies with user names, addresses, hometowns, and information through its other services. Second CAC at ¶91. Those DoubleClick cookies persist, and are read by Google when Plaintiffs visit other Google websites.

As with Facebook in the *Hulu* case, Google already has the corresponding data in its records to connect the DoubleClick cookie identifiers, UDIDs, and IP addresses to individual consumers. It does not have to collect information from any source other than itself. Google can cross-reference the values of the information disclosed by Viacom with other information in its databases to discover the identities of Nick.com users. Combined, these databases individually

[6] See http://www.google.com/policies/privacy/key-terms/#toc-terms-personal-info. Last visited Oct. 15, 2014 (emphasis added).

identify Internet users because the information is "in fact linked" to individuals in its collection and use by Google.

Viacom also argues that because Google promises not to combine the information obtained to identify individuals, Viacom has not disclosed personally identifiable information. Doc. 77-1, Viacom Memo. at 11. Although the VPPA contains specific exceptions in 18 U.S.C. § 2710(b)(2), there is no exception for disclosure to third-parties who promise not to connect information already within their control. Whether Google promises to take measures to prevent the linkage of the data it receives and the data it possesses bears no relevance to Viacom's obligations under the VPPA.

With the information disclosed by Viacom, Google knows the Plaintiffs' username/alias, gender, age, IP address, browser settings, unique device identifier, operating system, screen resolution, browser version, web communications, and the persistent cookie identifier which, along with the IP address and UDID, ties all of the information together. CAC at ¶143. This information does more than point, it identifies the Plaintiffs as individuals.

As a result, Plaintiffs adequately allege that Viacom disclosed personally identifiable information about Plaintiffs and their video-viewing histories to Google in violation of the VPPA.

II. PLAINTIFFS PROPERLY PLEAD CLAIMS UNDER THE NEW JERSEY COMPUTER RELATED OFFENSES ACT

Plaintiffs' Second Complaint sets forth sufficient facts to sustain their claim under the New Jersey Computer Related Offenses Act ("NJCROA"). The NJCROA provides a right of action for damages to any person (1) "damaged in business or property" as a result of (2) "purposeful and knowing" conduct prohibited by the Act. *See* N.J.S.A. § 2A:38A–3; *see also* Google's Motion, p. 11 ("To state a claim under the [NJ]CROA, Plaintiffs must allege that

[Defendants] (1) 'damaged [Plaintiffs] in business or property' by (2) engaging in enumerated conduct"). Plaintiffs' factual allegations, properly construed, are more than sufficient to support both elements of their claim. Nevertheless, Defendants assert two main grounds for dismissal. Defendants argue Plaintiffs fail to properly plead a viable theory of "business or property" damage. Second, Defendants argue Plaintiffs fail to allege facts showing Defendants engaged in conduct prohibited under the Act. On this point, Defendants complain that Plaintiffs fail to identify the data or information taken from their computers; that is, according to Defendants, Plaintiffs plead nothing more than unwanted "access" to information. With respect to their second argument, Defendants further assert dismissal is appropriate for the reason that Plaintiffs fail to plead facts showing Defendants acted with purpose or knowledge. *See* Viacom Motion, p. 21, n. 6.; Google's Motion, pp. 16-17.[7]

There is no merit to any of this. In their Second Complaint, Plaintiffs allege sufficient damages under a new theory that ties the NJCROA to unjust enrichment in a quasi-contractual setting. *See* Second Class Action Complaint ("Second Complaint") at ¶ 153. Additionally, Plaintiffs have pled the necessary facts, including purposeful or knowing conduct designed to alter, access and/or harvest data on Plaintiffs computers. In short, Plaintiffs' Second Complaint properly states a claim under the NJCROA. The Court should agree and so hold.

[7] In its motion, Google adds an additional attack on Plaintiffs' claim by adding another element to the NJCROA—"purposeful or knowing *harm*." According to Google, Plaintiffs fail to plead facts showing "Google's purpose was to injure Plaintiffs…." Google's Motion, pp. 16-17. As set forth in more detail below, there is nothing in the NJCROA that requires Plaintiffs to demonstrate purposeful or knowing *harm*, as opposed to purposeful or knowing *conduct*. Indeed, despite its statements to the contrary, Google implicitly acknowledged as much, stating Plaintiffs may properly state a claim under the NJCROA if they allege "that Google (1) 'damaged [Plaintiffs] in business or property' by (2) engaging in enumerated *conduct*." Google's Motion, p. 11.

a. PLAINTIFFS ALLEGE SUFFICIENT FACTS TO SHOW DAMAGE IN BUSINESS OR PROPERTY

The NJCROA states "[a] person or enterprise damaged in business or property as a result of any of the following actions may sue the actor therefor in the Superior Court . . . ." N.J.S.A. 2A:38A-3. Plaintiffs need not show the precise value of the damage caused because the NJCROA tasks a jury with that charge. *See* N.J.S.A. § 2A:38A-4 ("[t]he value of damage, loss, property or income involved in any lawsuit shall be determined by the trier of fact."). Thus, Plaintiffs need only point to some damage in business or property and need not allege specific value at this early stage in the proceedings.

The Second Complaint alleges that:

> Through conversion and without consent, Defendants harvested Plaintiffs' personal information for their unjust enrichment and to the financial detriment of Plaintiffs and Class Members. Had Plaintiffs, Class Members, and/or their parents and/or guardians known that Defendants were converting Plaintiffs' personal information for financial gain, Plaintiffs, Class Members, and/or their parents and/or guardians would have at least expected remuneration for their personal information at the time it was conveyed.

Second Complaint at ¶ 153.

Plaintiffs appreciate that these allegations include unjust enrichment language and that the Court dismissed Plaintiffs' independent unjust enrichment claim for the reason that New Jersey does not recognize it as an independent action in tort. July 2, 2014 Opinion at 38., citing *Goldsmith v. Camden County Surrogate's Office*, 975 A.2d 459, 462-63 (N.J. App. Div. 2009). Plaintiffs, however, present unjust enrichment not as an independent action in tort, but as a measure of damages under the NJCROA in a quasi-contractual sense. *See Goldsmith*, 975 A.2d at 463 (stating quasi-contracts permit unjust enrichment as available remedy).

In a quasi-contract "there is no agreement; but they are clothed with the semblance of contract for the purpose of the remedy, and the obligation arises not from consent, as in the case

of true contracts, but from the law or natural equity." *Callano v. Oakwood Park Homes Corp.*, 219 A.2d 332, 334 (N.J. App. Div. 1966). Usually, a contract defines the duty, but "in the case of quasi-contracts the duty defines the contract. Where a case shows that it is the duty of the defendant to pay, the law imparts to him a promise to fulfill that obligation. The duty which thus forms the foundation of a quasi-contractual obligation is frequently based on the doctrine of unjust enrichment." *Id.*

To show unjust enrichment a party must demonstrate "that it expected remuneration from the defendant at the time it performed or conferred a benefit on defendant and that the failure of remuneration enriched defendant beyond its contractual rights." July 2, 2014 Opinion at 38, citing *VRG Corp. v. GKN Realty Corp.*, 641 A.2d 519, 554 (N.J. 1994). A plaintiff need only show that if they had known all the facts "he would have expected remuneration from defendant. . . ." *Id.*, citing *Mu Signa, Inc. v. Affine, Inc.*, No. 12-cv-1323 (FLW), 2013 WL 3772724, at *10 (D.N.J. July 17, 2013).

Here, when the minor Plaintiffs first visited Nick.com, they were greeted by a picture of a smiling cartoon character, Sponge Bob Square Pants, and asked to enter information including their name, gender and date of birth. Second Complaint at ¶ 103. Right above the cartoon character, is the following language: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!" *Id.* (emphasis in original). The form itself belies this statement, as the form asks for Plaintiffs' personally identifiable information (PII) in the form of gender and birthdate. *Id.* Additionally, Plaintiffs allege the illegal harvesting, conveyance and use of Plaintiffs' IP address, browser settings, and video viewing histories. Second Complaint at ¶¶ 106-107. At the time that the minor Plaintiffs provided their PII, they had no way of knowing how the information would be

used. Had they known, and more importantly had their parents or legal guardians known, that Defendants would monetize their PII, Plaintiffs would not have provided their PII without compensation or would have at least had the option not to provide that information in the first place. Defendants, through nefarious business practices, hid this from Plaintiffs denying them of that choice.

Undoubtedly, Plaintiffs' PII has monetary value to Defendants.[8] So too does Plaintiffs' PII have value to Plaintiffs as this is part of the basis for the privacy interest alleged in the Second Complaint's intrusion upon seclusion claim. Had Plaintiffs known that the information they provided would be harvested and illegally conveyed to Defendants for advertising purposes, they would have had a choice not to send the information. As such, now Plaintiffs have no choice about what happens to the PII Defendants harvested and conveyed, but they should at least be compensated, and rightly would have expected compensation, for the benefit Defendants received. Thus, this Court should deny Defendants' motions because Plaintiffs have demonstrated an injury in business or property as required by the NJCROA.

b. PLAINTIFFS ALLEGE SUFFICIENT FACTS TO SHOW DEFENDANTS ENGAGED IN CONDUCT PROHIBITED BY N.J.S.A. 2A:38A-3(A-E).

Plaintiffs' Second Complaint further alleges all the necessary facts to show that Defendants engaged in conduct violating NJCROA subsections (a)-(c), and (e).[9] In that regard, the NJCROA prohibits:

---

[8] The precise amount attributed to that value is contested by both parties, but it is not important at this point in the proceeding. *See* N.J.S.A. § 2A:38A-4.

[9] Footnote 6 to Google's Motion alleges Plaintiffs did not respond to arguments regarding the subsections of N.J.S.A. 2A:38A-3 after its first Motion to Dismiss and as such should be waived. That is false. Plaintiffs' first Opposition spent several pages discussing the specific language of the statute's subsections and how Defendants' actions were in violation thereof. Plaintiffs' Opposition to Defendants' Motions to Dismiss the Master Complaint at 52-55. That Plaintiffs did not go through section by section with sub-point headings as Defendant Google does is

a. The purposeful or knowing, and unauthorized altering . . . of any data, database, computer program, computer software or computer equipment . . . ;
b. The purposeful or knowing, and unauthorized altering . . . of a computer . . . ;
c. The purposeful or knowing, and unauthorized accessing or attempts to access any computer . . . ;
d. The purposeful or knowing, and unauthorized altering . . . of a financial instrument; or
e. The purposeful or knowing accessing and reckless altering . . . of any . . . computer, computer program, computer software . . . .

N.J.S.A. 2A:38A-3. Here, Plaintiffs' Second Complaint alleges Defendants purposefully or knowingly altered and/or accessed Plaintiffs' computers without their consent. Second Complaint at ¶ 153. Thus, Plaintiffs have alleged all the elements of an NJCROA claim and Defendants' Motions should be denied.

i. Defendants' Actions Were Done Purposefully or Knowingly and with Intent to Alter or Access Plaintiffs' Computers

All of the subsections in N.J.S.A. 2A:38A-3 require purposeful or knowing altering or accessing of another's computer, *i.e.*, purposeful or knowing conduct. Plaintiffs' Second Complaint states:

> Immediately upon the Plaintiffs' first communication with Nick.com, Defendant Viacom automatically placed its own first-party cookies on the computing devices of the Plaintiffs. Additionally, immediately upon the Plaintiffs' first communication with Nick.com, Viacom knowingly permitted Defendant Google to place its own third-party cookies on the computing devices of the Plaintiffs and then transmitted the Plaintiffs' subsequent communications to Google through those persistent tracking cookies and other information . . . .

Second Complaint at ¶¶ 67-68. This was nothing unusual as the software cookies performed exactly as they had been intentionally and purposefully programmed to do. Defendants admit

---

immaterial. Plaintiffs certainly addressed all the relevant language in each sub-section to show Defendants' violations. The only subsection Plaintiffs did not specifically address is N.J.S.A. 2A:38A-3(d), which deals with "financial instruments" that are not at issue in this case.

throughout their briefs that this is just how internet advertising works.[10] *See* Google Motion at 3 (stating cookies are "widely used on the internet"); Viacom Motion at 13 (stating cookies are "well known features of the internet"). While the parties dispute the legality of this action, neither party disputes that the cookie programs utilized by Defendants did anything but work exactly as they were designed to by the Defendants.[11]

ii. Defendants Wrongfully Acquired Information and Data Through Their Purposeful or Knowing Access to Plaintiffs' Computers

In their motions, Defendants claim Plaintiffs have to specifically identify what data was taken, and they fault Plaintiffs for allegedly not doing so. *See, e.g.*, Viacom Motion, p. 18; *see also* Google Motion, p. 14. Though no such requirement exists in the statute, Plaintiffs have sufficiently alleged that Defendants illegally acquired Plaintiffs PII. *See e.g.* Second Complaint at ¶¶ 106-107 (noting Defendants harvested Plaintiffs' gender, birthdate, IP address, browser settings, and video viewing histories). Thus, Defendants' reliance on *PC Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504 (3rd Cir. 2005) and similar cases is misplaced. *PC Yonkers* was not decided at the motion to dismiss stage. Instead, it involved an appeal from the denial of a preliminary injunction, which was sought after at least some discovery had occurred. *See id.* at 507. More importantly, however, even with the benefit

[10] This is exactly the same argument that Goldman Sachs made when trying to defend its morally reprehensible actions in selling mortgage backed securities to its customers and then bet against those securities on the open market to make its customers bear the brunt of any loss. At the time, Goldman Sachs argued that its actions were legal and just how the stock market works. Just as in that example, Defendants morally abhorrent activity here should be found illegal even though Defendants' circular argument attempts to claim legality merely because it has always been done and never challenged in this way before.

[11] Imagine walking into a brick and mortar store and when you do an app installs on your phone, without your knowledge or consent, that mines your name, date of birth and gender. Then the store sends or sells that information to a third party and both begin sending you ads. This is exactly what Defendants do, just in a digital sense. It may be every day and ordinary to Defendants, but it is offensive and illegal to a customer under the NJCROA.

of discovery, the plaintiffs in that case did not know, nor could they show, what information, if any, had been taken. *Id.* at 509. And, according to the Court, access to the information alone was not enough to support a claim under the NJCROA. *Id.*; *see also PNC Mortg. v. Superior Mortg. Corp.*, No. 09-5084, 2012 WL 627995, at *5 (E.D. Pa. Feb. 27, 2012) (absence of "facts that show … data or information was taken" fatal to NJCROA claim). Here, however, Plaintiffs have not only alleged access to information, but they also identify what information was taken. In short, Plaintiffs' alleged facts are facially plausible and sufficient to support this element of their claim under the NJCROA.

iii. Plaintiffs Are Not Required To Plead or Prove Defendants Purposefully or Knowingly *Harmed* Plaintiffs

In its Motion, Google further argues Plaintiffs must show that "Google *purposefully or knowingly damaged Plaintiffs* in business or property." Google Motion at 16 (emphasis added). That is, according to Google, the NJCROA requires a plaintiff to demonstrate the defendant purposefully or knowingly caused *harm*.[12] Google's recitation of the law is incorrect. While the statute makes damage in business or property a prerequisite, it does not require that such damage be purposeful or knowing. N.J.S.A. 2A:38A-3. To the contrary, the NJCROA only applies to purposeful or knowing conduct; that is, the access or altering must be purposeful or knowing. Any damage need only flow from such conduct; it does not itself need to have been inflicted purposefully or knowingly. And, as described above, Defendants' actions in programming a cookie that automatically and without consent copied itself to Plaintiffs' computers, causing an

[12] In support of its argument, Google relies on comparisons to the CFAA and case law interpreting the same. *See, e.g.,* Google's Motion, pp. 16-17. The plain language of the NJCROA, however, is sufficient and requires no further clarification from sources in other statutes and jurisdictions. *See Lozano v. Frank De Luca Constr.*, 842 A.2d 156, 161 (N.J. 2004) (confirming "[w]e first look to the words of the statute, and if the language is clear, we interpret the statute consistent with its plain meaning.").

alteration to those computers, was purposeful and intentional satisfying these elements of any subsection of N.J.S.A. 2A:38A-3(a)-(c) and (e).

iv. Defendants' Actions were Unauthorized and Reckless

Subsections (a)-(c) of N.J.S.A. 2A:38A-3 all require that the action taken by Defendants was done without authorization. Plaintiffs' Second Complaint properly alleges that, "[t]he placement and/or access of these cookies occurred before either the Plaintiffs or their legal guardians had the opportunity to consent to their placement and access to the Plaintiffs' Internet communications." Second Complaint at ¶ 71. Additionally, Plaintiffs reiterate the argument outlined in Plaintiffs' Opposition to Defendants' First Motions to Dismiss that Plaintiffs are minors and legally incapable of consent, making Defendants' actions unauthorized. *See, J.D.B. v. N. Carolina*, 131 S.Ct. 2394, 2403-04 (2011) ("Like this Court's own generalizations, the legal disqualifications placed on children as a class— *e.g.,* limitations on their ability to alienate property, *enter a binding contract enforceable against them*, and marry without parental consent—exhibit the settled understanding that the differentiating characteristics of youth are universal.") (emphasis added); *Mechanics Fin. Co. v. Paolino,* 102 A.2d 784, 786 (N.J. App. Div. 1954) (stating that "[i]t is generally true that an infant may avoid his contract."); *Boyce v. Doyle,* 273 A.2d 408, 409-10 (N.J. Sup. Ct. 1971) (holding institution of legal action on behalf of minor is sufficient to operate as a rescission of contract signed by minor).

Additionally, subsection (e) of N.J.S.A. 2A:38A-3 requires "reckless altering . . . of any . . computer . . . ." Google claims nothing it did was reckless. Google's Motion, p. 16. But, Google knew that users of Nick.com were minor children who lack the capacity to consent to any agreement to place cookies on their computers. In ignoring this fact, Defendants' actions were at least reckless and, at worst, were knowingly and purposefully exploiting the web to prey

on unsuspecting and unsophisticated children. Thus, Plaintiffs have surpassed their burden under the remaining elements of the NJCROA and Defendants' motions should be denied.

III. INTRUSION UPON SECLUSION

The tort of intrusion upon seclusion imposes civil liability for invasion of privacy on "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." Doc. 65, Opinion, p. 36 (quoting *Hennessey v. Coastal Eagle Point Oil Co.*, 609 A.2d 11, 17 (N.J. 1992); Restatement (Second) of Torts, § 652B)). "The privacy invasion 'need not be physical'; indeed, it may arise from 'some other form of investigation or examination' into an individual's 'private concerns.'" *Id.* "To succeed with a claim for intrusion upon seclusion, a plaintiff 'must establish that he possessed a reasonable expectation of privacy' in the affairs or concerns intruded upon." *Id.* (quoting *G.D. v. Kenny*, 15 A.3d 300, 320 (N.J. 2011)).

In its Order on Defendants' initial Motion To Dismiss, the Court found that Plaintiffs' Complaint plausibly "alleges facts demonstrating that for purposes of New Jersey law Plaintiffs had a reasonable expectation that certain aspects of their online identities remain private and that Defendants intruded upon those private concerns." Doc. 65, p. 37. The Court found, however, that the Complaint failed to set forth sufficient facts alleging that the intrusion "would be highly offensive to a reasonable person" and dismissed the intrusion claim without prejudice to allow Plaintiffs to re-plead additional facts. *Id.* Plaintiffs have done so and submit that the Second Amended CAC sets forth facts sufficient to state a claim of Intrusion Upon Seclusion.

a. DEFENDANTS' INTRUSION WAS INTENTIONAL

Ignoring the Court's Order, Defendants again make the absurd circular argument that they can only violate the law if they know they are violating the law. Google Memo. p. 18; Viacom Memo. pp. 28-29. Defendants' argument must be rejected on several obvious grounds.

First, § 652B of the Restatement (Second) does not "require a complainant to have knowledge of the reasons for the intrusion. Rather, the intentional intrusion itself . . . is sufficient to establish these torts." *Yates v. Commer. Index Bureau, Inc.* 861 F. Supp. 2d 546, 551 (E.D. Pa. 2012). Second, the *knowing* commission of an illegal act is, by definition, highly offensive to a reasonable person. Defendants' inclusion of such a "scienter" requirement would, therefore, render the tort's "highly offensive" element meaningless. Third, the issue of Defendants' knowledge of the legality of its own conduct would require extensive fact-finding, making dismissal at this stage premature.[13]

Furthermore, the cases relied upon by Defendants, *O'Donnell v. United States*, 891 F.2d 1079 (3d Cir. 1989) and *Jevic v. Coca Cola Bottling Co. of N.Y., Inc.*, No. 89-4431, 1990 WL 109851 (D.N.J. 1990) do ***not*** establish that intrusions are permissible unless known by the intruder to be unlawful. Rather, these cases explain that "to intrude, in the tort context, one must act without permission." *Jevic*, 1990 WL 109851 at *8. In both *O'Donnell* and *Jevic*, there was no dispute of material fact that the defendants had permission to commit the intrusive acts, and, as a result, the intrusions were not actionable. *See O'Donnell*, 891 F.2d at 1081, 1083; *Jevic*,

[13] Accepting Defendants' argument would further create a need for discovery of attorney-client communications to thoroughly examine Defendants' knowledge of the legality of their actions. *See Payton v. New Jersey Turnpike Authority*, 691 A.2d 321 (N.J. 1997). ("'Although important,' in New Jersey, the [attorney-client] privilege is not sacrosanct. It 'may be pierced upon a showing of need, relevance and materiality, and the fact that the information could not be secured from any less intrusive source.'") (citing *In re Kozlov*, 398 A.2d 882 (1979)).

1990 WL 109851 at *9-10. *See also Gibbs v. Massey*, No., 07-3604, 2009 WL 838138, at *11 (D.N.J. March 26, 2009) ("The linchpin of the intrusion element is that it must be committed without consent.").

Here, Defendants did not receive, or even seek, consent from Plaintiffs or their parents prior to deliberately gathering the personal information of millions of young children.[14] Even if these children had voluntarily provided their usernames and registration information (assuming that young children may be said to do so voluntarily), neither Plaintiffs nor their parents authorized Defendants to intercept, track, record, and disseminate their personal information or the content of their Internet communications. These actions by Defendants are strikingly similar to the illustrations of actionable intrusions described in §652B of the Restatement, and cited in *O'Donnell*—"wiretapping a person's phone or using binoculars to view inside a private residence." *See O'Donnell*, 891 F.2d at 1083 n.3.

Finally, Google argues that its purpose in collecting this information was to make money and, thus, not illegal. Google Memo. p. 18. The intruder's subsequent use of the information obtained, however, does not bear on whether an unlawful intrusion occurred: "The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information obtained." *Bisbee v. John C. Conover Agency, Inc.*, 452 A.2d 689, 691 (N.J. Super. Ct. App. Div. Oct. 20, 1982) (quoting 3 Restatement of Torts 2d, §652B, comment b at 378-79).

[14] Defendant Viacom changed its sign-up process soon after Plaintiffs filed suit so that they no longer required registered users at Nick.com to give their precise birthdate. Second CAC at ¶103, n.38. More recently, Viacom appears to have severed its relationship with the Google DoubleClick cookies. Second CAC at ¶148.

Accordingly, as reflected in the Court's prior Order, Plaintiffs have adequately alleged that Defendants committed intentional intrusions, as follows:

- Intentionally accessing, storing, and utilizing without consent the personally identifiable information of children, such as: (1) the child's username/alias, (2) the child's gender, (3) the child's birthdate, (4) the child's IP address, (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's Nick.com website; and (11) the DoubleClick persistent cookie identifiers (Second CAC at ¶¶109-114, 143);

- Knowingly disclosing and obtaining without consent the personally identifiable information of children, including the contents of the children's electronic communications and video materials requested and obtained (Second CAC at ¶¶145-147);

- Deliberately disclosing the personal information of children to Google with knowledge of Google's ubiquity and ability to identify Internet users via the information disclosed (Second CAC at ¶¶95-96);

- Intentionally accessing, attempting to access, tampering with, altering, damaging, taking, destroying, obtaining and/or intercepting the children's computer, computer software, data, database, computer program, computer system, computer equipment and/or computer network (Second CAC ¶ 152); and

- Intentionally taking the children's information from the privacy of their homes without their consent or the consent of their legal guardians (Second CAC ¶ 158).

b. DEFENDANTS' UNAUTHORIZED INTRUSION INTO THE PRIVATE MATTERS OF CHILDREN WAS HIGHLY OFFENSIVE

i. The Legal Standard

To establish liability for the tort of intrusion upon seclusion, "a plaintiff must show that 'the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object.'" *Castro v. NYT Television*, 895 A.2d 1173, 1177 (N.J. App. Div. 2006) (*citing Restatement (Second) of Torts* § 652B cmt. b).

Whether an intrusion is highly offensive "turns on what a person's reasonable expectation of privacy is with respect to the item or area searched or intruded upon." *Torsiello v. Strobeck*, 955 F. Supp. 2d 300, 315 (D.N.J. 2013) (*citing White v. White*, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001); *State v. Hempele*, 576 A.2d 793 (N.J. 1990) (holding that "expectations of privacy are established by general social norms")). Courts then "weigh the competing interests of the parties to determine whether the defendant's reasons for its intrusion outweigh the plaintiff's right to privacy." *Id.* (*citing N.O.C., Inc. v. Schaefer*, 484 A.2d 729 (N.J. Super. 1984); *Parish Nat'l Bank v. Lane*, 397 So.2d 1282 (La. 1981)).

Determining whether an intrusion is "highly offensive to a reasonable person is a question of fact for the jury to decide." *Desmond v. Phillips & Cohen Assocs.*, 724 F. Supp. 2d 562, 569 (W.D. Pa. 2010); *see also Vurimindi v. Fuqua Sch. of Bus.*, 435 Fed. Appx. 129, 136 (3d Cir. 2011) (unpublished) (reversing district court's dismissal of intrusion upon seclusion claim which alleged defendants, *inter alia*, monitored his computer)[15] (*citing Toomer v. Garrett*, 574 S.E.2d 76, 90 (N.C. Ct. App. 2002) ("The kinds of intrusions that have been recognized under this tort include 'physically invading a person's home or other private place, eavesdropping by wiretapping or microphones, peering through windows, persistent telephoning, unauthorized prying into a bank account, and opening personal mail of another.'"); *Dalley v. Dykema Gossett*, 788 N.W.2d 679 (Mich. App. 2010) ("Whether a reasonable person would find an intrusion objectionable constitutes a factual question best determined by a jury."); *Ruzicka Elec. & Sons, Inc. v. IBEW*, 427 F.3d 511 (8th Cir. 2005) ("Whether a defendant obtained

[15] As Google points out, "Pennsylvania common law [on the tort of intrusion] is virtually identical to New Jersey common law." Google Memo. pp. 17-18 n.9 (*quoting Rush v. Portfolio Recovery Assocs. LLC*, 977 F. Supp. 2d 414, 433 n.23 (D.N.J. 2013).)

information through a method objectionable to the reasonable person is 'ordinarily a question for the jury.'").

A determination that conduct is highly offensive "only becomes a question of law if reasonable persons can draw only one conclusion from the evidence." *Remsburg v. Docusearch*, 816 A.2d 1001, 1008 (N.H. 2003). Thus, the burden is on Defendants to show that the conduct complained of is such that "reasonable persons can draw only one conclusion" from the facts in the pleadings which, at this stage, must be "accepted as true and viewed in the light most favorable to the plaintiff."

ii. Social Norms Establish Plaintiffs' Reasonable Expectation Of Privacy In The Information Obtained And Disseminated By Defendants

As set forth above, "[e]xpectations of privacy are established by general social norms," *Hempele*, 576 A.2d 793. Here, Plaintiffs allege that Defendants intruded into their personal information and communications. Plaintiffs had an expectation of privacy in this information derived from general social norms embodied in various sources of public policy, including, constitutional and legislative enactments, common law principles, and industry standards.

The United States Constitution provides the most basic evidence of "social norms," serving as "a national expression of public policy, a moral compass to help us focus on the values that are at stake in this case." *Soliman v. Kushner Companies, Inc.*, 77 A.3d 1214, 1223-24 (N.J. App. Div. 2013). The New Jersey Supreme Court "has acknowledged that the right to privacy is 'grounded' in the Fourteenth Amendment of the United States Constitution's concept of 'personal liberty. . . . [which] safeguards at least two different kinds of interests: 'the individual interest in avoiding disclosure of personal matters,' and 'the interest in independence in making certain kinds of important decisions.'" *Id.* at 1223. This reasonable expectation of privacy is "a most fundamental human right," "the most comprehensive of rights," "the right

most valued by civilized men," and one that is "older than the Bill of Rights – older than our political parties, older than our school system." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 487 (1974), *Olmstead v. United States*, 277 U.S. 438, 478 (1928), *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965). In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court unanimously held that Americans have a right to privacy in the data contained on personal computing devices, and it expressed particular concern for the privacy of "Internet search and browsing history." *Id.* at 2489-90.

As this Court has noted, "the right to privacy created by Article I, Paragraph 7 of the New Jersey constitution provides greater protection than the privacy right created by the federal Constitution." Doc. 65, p. 36 (citing *State v. Reid*, 945 A.2d 26, 32-34 (N.J. 2008)). "New Jersey 'explicitly recognizes a right to 'informational privacy,' which encompasses any information that is identifiable to an individual.'" *Id.* (citing *State. v. Reid*, 914 A.2d 310, 314 (N.J. Sup. Ct. App. Div. 2007); *Doe v. Poritz*, 662 A.2d 367, 412 (N.J. 1995) ("We have found a constitutional right of privacy in many contexts, including the disclosure of confidential or personal information."). "'Personal information [is] any information, no matter how trivial, that can be traced or linked to an identifiable individual.'" *Id.* (quoting *Reid*, 914 A.2d at 314).

Civil and criminal statutes also evidence social norms of "highly offensive" behavior supporting a claim for intrusion upon seclusion. *See, e.g.*, *Latture v. Emmerling*, No. 304833, 2013 WL 5225243, at *4 (Mich. App. 2013) ("Criminal activity is an objectionable method of obtaining information."); *Clayton v. Richards*, 47 S.W.3d 149, 154 at n. 1 (Tex. App. 2001) ("Unlawful interception of wire, oral, or electronic communications is a criminal act under [Texas law]. Courts further give weight to the fact that conduct is a crime when determining if it also amounts to a tort." (citing Dan B. Dobbs, The Law of Torts § 2 (2000))); *Nader v. General*

Motors Corp., 25 N.Y.2d 560 (N.Y. App. 1970) ("[T]o the extent the two challenged counts charge it with wiretapping and eavesdropping, an actionable invasion of privacy has been stated."); *see also*, *inter alia*, the Video Privacy Protection Act, the Wiretap Act, the Pen Register Act,[16] the Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states.

Finally, nowhere are these social norms clearer than with young children, whom the Supreme Court has recognized "have a very special place in life which law should reflect." *May v. Anderson*, 345 U.S. 528, 536 (1953). According to the Supreme Court, children are entitled to enhanced protection under the law precisely because: (1) children possess "peculiar vulnerability"; (2) children are unable "to make critical decisions in an informed, mature manner"; and (3) of the "importance of the parental role in child rearing." *Belotti v. Baird*, 443 U.S. 622, 635 (1979). Recognizing these interests, Congress enacted the Children's Online Privacy Protection Act ("COPPA") in 1998 to protect against the collection of personal information over the internet from children under the age of 13. *See* 15 U.S.C. §§ 6501-06. These social norms are also reflected in Defendants' own industry, which has established Terms of Use and other standards protecting young children from the collection and disclosure of personal information.

---

[16] Information that includes "content" is protected by the Wiretap Act, while "dialing, routing, addressing, or signaling" information ("DRAS") is protected by the Pen Register Act. *See* 18 U.S.C. § 3127. While a URL may be both "content" and DRAS, *see NSA Declassified Opinion 2* at 32 (*available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf), there is agreement that URLs, IP addresses, UDIDs, and persistent cookie identifiers contain DRAS. *See, e.g.*, *In re: Application of the U.S. for an Order Authorizing Use of a Pen Register and Trap on [xxx] Internet Service Acc't*, 396 F.Supp. 45, 58 (D. Mass 2005) (holding that IP addresses are DRAS which may be tracked via a pen register with court permission). As such, Defendants' conduct, at minimum, involved the recording of DRAS without consent in violation of the Pen Register Act.

Here, Plaintiffs allege that the information obtained and disclosed by Defendants is "personal information" subject to an expectation of privacy because it can be traced or linked to identifiable individuals. *See* Second CAC ¶¶ 78-94. Consistent with the established social norms described above, the Second CAC alleges that Defendants, without seeking or obtaining the permission of Plaintiffs or their parents, invaded the privacy rights of millions of children under the age of 13 by obtaining, tracking, and disclosing personal information and Internet communications from the privacy of their homes, including the following: (1) the child's username/alias, (2) the child's gender, (3) the child's birthdate, (4) the child's IP address, (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's Nick.com website; and (11) the DoubleClick persistent cookie identifiers. Second CAC at ¶¶78-94, 109-114, 143-147, 152, 158, 162, 165. Plaintiffs further allege that Defendant Viacom discloses this information to Google knowing Google's ubiquity and ability to use the information to identify individuals. Second CAC at ¶¶78-94, 143-145. In addition, Plaintiffs allege that Defendants placed significantly more tracking technologies on children's websites than adult websites to take advantage of the Plaintiffs' vulnerability as children. Second CAC at ¶¶ 56, 166. Thus, Plaintiffs allege that Defendants obtained and disclosed personal information and Internet communications knowing it could be traced or linked to identifiable young children. Second CAC at ¶¶ 78-94, 144-146.

As Plaintiffs allege, given the special place of children in society, a reasonable person could find Defendants' unauthorized intrusions into the private matters of children under the age of 13 are highly offensive because they exploit the vulnerability of children and disregard the

importance of the parental role. Moreover, based on Defendants' unauthorized collection and disclosure of information that can be traced or linked to an identifiable individual, a reasonable person could find Defendants' intrusions highly offensive because they violate the social norms embodied in the "informational privacy" and confidential/personal information protections of the New Jersey Constitution, and fly in the face of a "most fundamental human right" enshrined in the U.S. Constitution.

Plaintiffs further allege that Defendants' intrusions are highly offensive because they violate the social norms embodied in: (1) the Terms of Use[17] of Plaintiffs' Internet Service Providers and web-browsers,[18] which prohibit the use of those services in criminal activity, unlawful activity, and the tracking of Internet communications without consent; and (2) the standards of the online advertising industry, including the Interactive Advertising Bureau's Code of Conduct, in which Defendants agreed to "not collect 'personal information' as defined in the Children's Online Privacy Protection Act ('COPPA') from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising." Second CAC at ¶¶137b, 163, 167.

In addition, Plaintiffs allege that Defendant Viacom's intrusions are highly offensive because they violate the social norms embodied by the Video Privacy Protection Act, the

---

[17] *See* Second CAC at ¶¶65-66 for links to relevant Terms of Use of the most popular Internet Service Providers and web-browsers.

[18] Contrary to Google's factual argument that it is a service provider not subject to the Terms of Use, Google is not actually an ISP. Instead, websites like Nick.com (and DoubleClick.com) are "users" of electronic communication services like ISPs and web-browsers. *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (Amazon.com a user, not provider of ECS).

Wiretap Act,[19] the Pen Register Act,[20] the Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states. Second CAC at ¶160. For example, the Computer Fraud and Abuse Act prohibits: (1) intentional access to a computer (2) without authorization or exceeding authorized access, and (3) thereby obtaining information from a protected computer. 18 U.S.C. § 1030(a)(2)(C). Defendants argue Plaintiffs have simply made a conclusory statement that they violated the CFAA; however, Plaintiffs allege that Defendants intentionally accessed Plaintiffs' computers by placing tracking cookies on them and utilized those tracking cookies to intercept and record the Plaintiffs' personal information and communications without authorization and with knowledge that the Plaintiffs were minor children. Second CAC ¶¶ 5-6, 67-72, 76-77, 102-114, 137, 143-146. Such conduct violates the elements of the CFAA set forth above. Second CAC ¶ 160d. The fact that the CFAA and laws in every state provide criminal penalties to Defendants' alleged conduct supports the plausibility of Plaintiffs' allegations that Defendants' conduct is "highly offensive" to a reasonable person.[21]

Finally, with regard to Defendants' burden of establishing that no reasonable juror could find their conduct offensive, Plaintiffs allege facts showing: (1) eighty-six percent of Americans oppose the practice of advertisers tracking "a child's behavior online even if they give the child free content"; (2) eighty percent oppose the tracking of children even where an advertiser does

---

[19] Both Defendants point out that this Court previously ruled against Plaintiffs' Wiretap claim. Plaintiffs plead this in the alternative for purposes of potential appeal.

[20] Defendant Viacom argues, without any legal authority, that the Pen Register Act does not apply to private parties. If the Act did not apply to private actors, the exceptions section in 18 U.S.C. § 3121(b) would be superfluous.

[21] Contrary to Viacom's assertion, the CFAA's creation of a statutory cause of action does not negate any common law cause of action. *See Lane v. CBS Broadcasting*, 612 F. Supp. 2d 623, 632 (E.D. Pa. 2009) ("Since [Defendant's] conduct clearly violates [CFAA] § 1030, Plaintiff could certainly pursue civil remedies under § 1030(g). However, Plaintiff is not required to do so." She may also "[choose] to seek relief under state law[.]"). Here, Plaintiffs' decision not to bring a CFAA claim is by no means a concession that Plaintiffs cannot state a CFAA claim.

not "know a child's name and address"; (3) ninety-one percent believe advertisers should receive a parent's permission before placing tracking software on a minor child's computing device; and (4) ninety percent support federal law requiring parental permission before the collection of personal information of a minor child online. Second CAC at ¶164.[22]

iii. Defendants' Commercial Interests In Making Money Do Not Outweigh Plaintiffs' Right To Privacy

Google incorrectly makes a factual argument that tracking the Internet communications of minor children without consent is "socially useful" and, therefore, outweighs Plaintiffs' privacy interests. Google Memo. p. 23. The fact that Defendants engage in the tracking and trafficking of children's Internet use for the purpose of making a profit, however, does not make such behavior "socially useful." Commerce existed prior to the invention of cookie tracking. It will continue to exist in socially useful ways if Defendants no longer track children's Internet use, as evidenced by the fact that Defendant Viacom has already stopped allowing Google to track its child users. Second CAC at ¶148. Reasonable people may disagree whether Defendants' tracking, collection, and disclosure of children's private information is "socially useful" and, if so, whether that makes Defendants' conduct less offensive.

Plaintiffs have plausibly alleged that Defendants' intrusions into the private matters of young children are highly offensive to a reasonable person. Defendants' motions to dismiss on

---

[22] Google argues the survey results must be ignored by this Court because "Plaintiffs allege no facts regarding the methodology by which the surveys were conducted or any other information to support their reliability." Google Memo. p. 22. In support, Google cites *Brokerage Concepts v. United States Healthcare*, a case in which the Third Circuit disregarded survey evidence ***presented by a litigant at trial*** in an anti-trust case under the hearsay rule. In a Rule 12(b)(6) motion, Plaintiffs are entitled to have all of their pleaded facts taken as true without proving their admissibility under the hearsay rule. Moreover, the Second CAC contains references to the source of each poll, where the Court can review the basic survey methodology. At this stage, however, Plaintiffs need not show the polls are fully admissible evidence.

the ground that no reasonable juror could find Defendants' conduct highly offensive should, therefore, be denied.

CONCLUSION

For all of the reasons stated herein, Plaintiffs respectfully request that this Court deny the Defendants' Motions to Dismiss.

Respectfully submitted,

/s/ Barry R. Eichen
Barry R. Eichen
Evan J. Rosenberg
EICHEN CRUTCHLOW ZASLOW & McELROY, LLP
40 Ethel Road
Edison, NJ 08817
732-777-0100
732-248-8273 Fax
beechen@njadvocates.com
erosenberg@njadvocates.com

/s/ James P. Frickleton
James P. Frickleton
Edward D. Robertson III
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
11150 Overbrook Rd., Suite 200
Leawood, KS 66211
913-266-2300
913-266-2366 Fax
jimf@bflawfirm.com
krobertson@bflawfirm.com

/s/ Edward D. Robertson, Jr.
Edward D. Robertson, Jr.
Mary D. Winter
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
573-659-4454
573-659-4460 Fax
chiprob@earthlink.net

marywinter@earthlink.net

Co-Lead Counsel on behalf of Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**MDL No. 2443**
	Docket No. 2:12-cv-07829 (SRC)(CLW)
This Document Relates to:	**CERTIFICATE OF SERVICE**
All Actions	

I HEREBY CERTIFY that on November 20, 2014, I caused the following documents to be electronically filed with the United States District Court for the District of New Jersey through the CM/ECF system on behalf of Plaintiffs:

a. Plaintiffs' Opposition to the Defendants' Motions to Dismiss; and
b. Certificate of Service.

The aforementioned documents were electronically filed with the Court and served on the following counsel of record through the CM/ECF system:

Stephen M. Orlofsky
BLANK, ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540
orlofsky@blankrome.com

Bruce P. Keller
Jeffrey S. Jacobson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022
bpkeller@debevoise.com
jsjacobs@debevoise.com

ATTORNEYS FOR DEFENDANT VIACOM, Inc.

Jeffrey J. Greenbaum
SILLS CUMMIS & GROSS PC
One Riverfront Plaza
Newark, NJ 07102-5400

jgreenbaum@sillscummis.com

Colleen Bal
Michael H. Rubin
WILSON SONSINI GOODRICH & ROSATI, PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105-1126
cbal@wsgr.com
mrubin@wsgr.com

Tonia O. Klausner
WILSON SONSINI GOODRICH & ROSATI, PC
1301 Avenue of the Americas, 40th Floor
New York, NY 10019
tklausner@wsger.com

ATTORNEYS FOR GOOGLE, INC.

Khaldoun Baghdadi
WALKUP MELODIA KELLY & SCHOENBERGER
650 California Street
San Francisco, CA 94108

Thomas Rosenfeld
GOLDENBERG HELLER ANTOGNOLI & ROWLAND PC
2227 South State Route 157
Edwardsville, IL 62025

Adam Voyles
LUBEL VOYLES LLP
5200 Montrose Blvd., Suite 800
Houston, TX 77086

Douglas Campbell
CAMPBELL & LEVINE LLC
1700 Grant Building
Pittsburgh, PA 15219

Jay Barnes
BARNES & ASSOCIATES
219 East Dunklin St.
Jefferson City, MO 65101

Andrew Lyskowski
BERGMANIS LAW FIRM LLC

380 West US Highway 54, Suite 201
Camdenton, MO 65020

PLAINTIFFS' STEERING COMMITTEE

Pursuant to 28 U.S.C. § 1746, I certify under penalty of perjury that the foregoing is true and correct.

Date: November 20, 2014

By: /s/ Evan J. Rosenberg

Barry R. Eichen
Evan J. Rosenberg
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

James P. Frickleton
Edward D. Robertson III
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
11150 Overbrook Rd., Suite 200
Leawood, KS 66211
Telephone: (913) 266-2300
Facsimile: (913) 266-2366

Edward D. Robertson, Jr.
Mary D. Winter
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
Facsimile: (573) 659-4460

Co-Lead Counsel on behalf of Plaintiffs